# Blockchain-Enabled Federated Learning: A Hyperledger Fabric Approach for Secure IoT Systems

Meysam Safari
*School of Electrical and Computer Engineering, College of Engineering*
*University of Tehran*
Tehran, Iran
me.safari@ut.ac.ir

Negar Rezaei
*School of Electrical and Computer Engineering, College of Engineering*
*University of Tehran*
Tehran, Iran
negar.rezaei@ut.ac.ir

Ahmad Khonsari
*School of Electrical and Computer Engineering, College of Engineering*
*University of Tehran,*
*School of Computer Science*
*Institute for Research in Fundamental Sciences(IPM)*
Tehran, Iran
a_khonsari@ut.ac.ir

2025 29th International Computer Conference, Computer Society of Iran (CSICC) | 979-8-3315-2311-4/25/$31.00 ©2025 IEEE | DOI: 10.1109/CSICC65765.2025.10967432

***Abstract*—The rapid growth of IoT devices necessitates robust solutions to ensure data privacy and security in distributed learning environments. This paper proposes a novel framework combining federated learning with Hyperledger Fabric blockchain to enable decentralized model training while safeguarding sensitive data. By leveraging blockchain's immutability and auditability alongside federated learning's data localization, the system establishes a secure and transparent ecosystem for collaborative machine learning. The paper details the system architecture, implementation strategies, and integration challenges, offering a practical solution for secure, privacy-preserving learning in IoT environments and highlighting the potential of blockchain-enabled federated learning for decentralized, data-sensitive applications.**

***Index Terms*—Blockchain, Federated Learning, IoT, Hyperledger Fabric, Privacy, Security**

## I. Introduction

The rapid expansion of the Internet of Things (IoT) has led to an unprecedented increase in the volume and variety of data generated by connected devices. [1] This data holds immense value for machine learning (ML) applications, providing innovation and enabling more efficient operations across various industries. However, the centralized collection and processing of sensitive IoT data pose significant risks to user privacy and system security. Centralized models are vulnerable to private data leaks and unauthorized access, which can result in privacy violations and compromised data integrity. [2] These challenges underscore the need for secure, privacy-preserving approaches to ML in IoT systems.

Federated learning (FL) has emerged as a promising technique to address these concerns by enabling decentralized model training directly on devices. In FL, individual devices train a shared ML model collaboratively without transferring raw data to a central server, thereby enhancing privacy. However, FL still faces challenges related to trust, model integrity, and secure coordination among participating devices. [3] A decentralized, auditable framework is essential to enhance FL's security guarantees and ensure reliable model updates, especially in sensitive IoT environments.

With its decentralized and immutable nature, blockchain technology offers a robust solution for securely coordinating federated learning in IoT networks. By combining blockchain and FL, we can create a transparent, tamper-resistant environment that maintains data privacy while ensuring the integrity of model training processes. [4] [5] Hyperledger Fabric, a permissioned blockchain platform, is particularly well-suited for this integration, providing features like data privacy, access control, and secure transaction management tailored for enterprise applications. [6]

This paper proposes a novel architecture that integrates federated learning with Hyperledger Fabric to create a secure, decentralized ML framework for IoT applications. Our approach leverages the transparency and auditability of blockchain to coordinate and verify federated learning updates across participating devices. We discuss the design and implementation of the system, including the integration of federated learning algorithms within Hyperledger Fabric, and demonstrate its ability to enhance privacy and security while maintaining scalability and performance.

To evaluate the effectiveness of the proposed framework, we conducted simulations under varying conditions, including different transaction arrival rates and network sizes. The evaluation focused on key performance metrics, such as latency, throughput, and scalability, to analyze the impact of integrating federated learning with blockchain in IoT networks. The results demonstrate that the integration of blockchain enhances the security and auditability of the learning process while maintaining acceptable levels of performance. Additionally, we provide insights into optimizing system parameters to reduce overhead and improve responsiveness.

The remainder of this paper is organized as follows: Section II reviews related work on federated learning, blockchain

technologies, and their integration for secure IoT systems, highlighting the gaps addressed by our approach. Section III presents the proposed system model and problem statement, providing details on the architecture, components, and mechanisms used to integrate federated learning with Hyperledger Fabric. Section IV evaluates the proposed system, including a privacy analysis demonstrating its security features and an experimental analysis to assess its performance under various configurations. Finally, Section V concludes the paper and outlines potential directions for future research, emphasizing areas for further optimization and real-world application.

## II. Related Work

The convergence of federated learning (FL) and blockchain technology has gained considerable attention as a solution for addressing privacy and security challenges in IoT networks. This section reviews recent advances in federated learning for IoT, the role of blockchain in decentralized data security, and previous attempts at combining FL with blockchain for secure model training.

**Federated Learning for IoT Privacy and Security:**

Federated learning has emerged as an effective approach for decentralized machine learning, particularly in environments like IoT, where devices generate large volumes of potentially sensitive data. FL enables local model training on individual devices, eliminating the need to centralize raw data, which helps mitigate privacy risks. Recent works by [3] and [7] have highlighted the privacy advantages of FL by keeping data on edge devices, thus reducing the attack surface for data breaches. However, implementing FL in IoT networks comes with its own challenges, including communication efficiency, model update verification, and security against adversarial model updates [8].

Moreover, federated learning in IoT faces trust issues, as device-generated model updates can be manipulated or compromised, potentially degrading the quality and integrity of the global model. Differential privacy and secure aggregation techniques have been proposed to mitigate some of these risks, but they do not fully address trust and auditability across devices [9]. These limitations highlight the need for a robust system that can verify updates and ensure reliable coordination among distributed devices in the absence of a central authority.

**Blockchain as a Solution for Secure Coordination in IoT:**

Blockchain has been extensively researched as a solution for securing decentralized environments, offering a tamper-proof ledger that can authenticate and verify transactions. In IoT networks, blockchain can improve data integrity, transparency, and accountability by ensuring that interactions between devices are verifiable and traceable. Traditional public blockchains, such as Bitcoin or Ethereum, offer high transparency, but they lack the privacy and scalability required for IoT applications [10]. Hyperledger Fabric, a permissioned blockchain, has been identified as a more suitable solution for enterprise-level IoT applications, as it allows for controlled access and private channels, which improve both privacy and efficiency [6].

Recent studies have utilized Hyperledger Fabric in IoT to establish secure access control and data logging mechanisms [11], which are essential for ensuring that only authorized devices are permitted to access or contribute to private data. This permissioned blockchain framework provides a flexible and scalable environment, making it a strong candidate for IoT applications that require both security and performance.

**Integrating Federated Learning and Blockchain for IoT:**

Integrating FL with blockchain has been explored as a solution for creating secure, privacy-preserving IoT networks. In this hybrid approach, blockchain can verify the authenticity of model updates and maintain a transparent log of all contributions, which enhances trust in the federated learning process. Recent research by [12] demonstrates the potential of combining FL with blockchain for reliable model training in IoT environments by using blockchain to log each model update transaction, thus creating a traceable record of contributions from each participant. Additionally, [13] explored the use of smart contracts to enforce policies for model updates, ensuring that only verified contributions are accepted into the global model.

Despite these advances, most existing studies employ public or consortium blockchains, which can introduce privacy risks and scalability limitations unsuitable for IoT. Our approach uses Hyperledger Fabric, a permissioned blockchain framework, to provide both privacy and scalability. By leveraging Hyperledger Fabric's modular structure and secure access control, our solution addresses the specific needs of federated learning in IoT, providing a secure, auditable, and efficient framework for decentralized model training. A comparative analysis of our proposed model with some state-of-the-art solutions is presented in Table I.

## III. System Model and Problem Definition

### A. System Model

1. Overview of the Architecture

Our proposed system integrates federated learning (FL) with the Hyperledger Fabric blockchain framework to enable secure and privacy-preserving machine learning within an IoT environment. This architecture is designed to support decentralized model training across distributed IoT devices, ensuring that sensitive data remains local. By leveraging blockchain, the system facilitates collaborative learning, maintaining data integrity and trust among participants. A visual representation of the proposed architecture is provided in Fig. 1.

The primary components of our system include:

- **IoT Devices:** These edge devices, operating within the scope of different organizations, act as local data collectors and model trainers, performing computations on-site without sharing raw data with a central entity.
- **Federated Learning Service:** This external service coordinates the training process by aggregating model updates from individual participants, allowing global model improvement without centralizing data.

**TABLE I:** Comparative Analysis of Proposed Model with State-of-the-Art Solutions

| Study | Technology | Blockchain Type | FL Integration | Security Features | Challenges Addressed |
|---|---|---|---|---|---|
| Nguyen et al. [3] | Federated Learning | Not Applicable | Yes | Privacy Preservation | Communication Efficiency |
| Khan et al. [7] | Federated Learning | Not Applicable | Yes | Edge Device Privacy | Adversarial Model Updates |
| Zhang et al. [8] | FL with Blockchain | Public Blockchain | Partial | Tamper Resistance | Trust Among Devices |
| Lu et al. [12] | FL with Blockchain | Consortium Blockchain | Partial | Update Verification | Model Integrity and Auditability |
| Kalapaaking et al. [13] | FL with Smart Contracts | Public Blockchain | Partial | Policy Enforcement | Scalability and Privacy Risks |
| **Proposed Model** | FL with Hyperledger Fabric | Permissioned Blockchain | Full | Data Integrity, Auditability, Privacy | Scalability, Trust, Secure Updates |

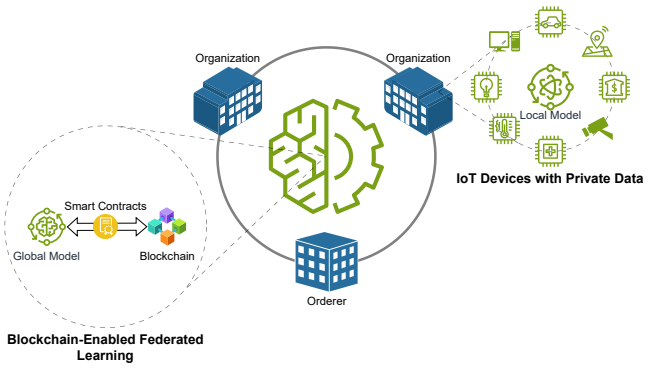


**Fig. 1:** Proposed Blockchain-Enabled Federated Learning Architecture

- **Blockchain Network:** The Hyperledger Fabric blockchain network serves as the backbone for secure communication, this permissioned blockchain manages transactions, maintains a tamper-proof log of model updates, and ensures that only authorized entities participate in the learning process.

2. Components of the System Model

1) **IoT Device Layer**
   In our model, each IoT device collects local data and trainings are performed on this data, generating model updates that reflect its local environment. These devices are responsible for periodically sending these updates to the federated learning aggregator. Importantly, the IoT devices never share raw data, addressing privacy concerns typical in traditional machine learning approaches.
2) **Federated Learning Service**
   The federated learning service is an external Python-based component designed to aggregate model updates from multiple devices. It employs various privacy-preserving federated learning techniques during the aggregation process. After aggregation, the updated global model is sent back to the IoT devices for further training iterations. Additionally, logs of various operations are recorded on the blockchain ledger to ensure security, auditability, and traceability.
3) **Hyperledger Fabric Blockchain Network**
   Hyperledger Fabric is the permissioned blockchain framework used to maintain the integrity, auditability, and transparency of the federated learning process. Each IoT device and the federated learning service function as nodes within the Fabric network, allowing them to interact securely through authenticated transactions.
   Key roles of the blockchain network include:

- **Authentication:** Using Fabric's membership service, the network authenticates all participants, ensuring only registered IoT devices can contribute updates.
- **Transaction Logging:** Each participant's activity, including model update transactions, is recorded on the blockchain, creating an immutable record that can be audited to verify contributions and activities from each IoT device.
- **Smart Contracts (Chaincode):** Smart contracts are deployed to automate the model update process, enforce update policies, validate the format of updates, and prevent malicious or unqualified data from entering the training process.

3. Workflow of the System Model

1) **Model Initialization:** The global model is initialized on the federated learning service and shared with each IoT device participating in the learning process.
2) **Local Training and Update Submission:** The local models are trained on IoT device data, and the resulting model updates are submitted to the blockchain.
3) **Verification and Aggregation:** The blockchain verifies each update transaction through consensus, and verified updates are aggregated by the federated learning service to form a new global model.
4) **Global Model Update:** The updated global model is then sent back to each IoT device for further training, continuing the iterative learning cycle.

### *B. Problem Statement*

The expansion of IoT networks poses significant privacy and security challenges, with centralized systems vulnerable to data breaches, tampering, and unauthorized access. While Federated Learning (FL) decentralizes training, it lacks update verification and trust mechanisms, leaving it vulnerable to attacks like model poisoning and unauthorized contributions.

To address these issues, this study integrates FL with Hyperledger Fabric, a permissioned blockchain framework. By leveraging blockchain's tamper-proof and transparent features, the system provides secure model updates, participant authentication, and policy enforcement through smart contracts, enabling a scalable and privacy-preserving federated learning solution for IoT.

## IV. Evaluation

### A. Privacy Analysis

Integrating Federated Learning (FL) with Hyperledger Fabric provides significant privacy enhancements by ensuring that sensitive user data remains localized and never leaves the IoT devices. This section analyzes the privacy implications of the proposed framework and presents a mathematical proof to demonstrate the privacy guarantees.

*1) Privacy Model:* In our framework, we adopt an *honest-but-curious* adversarial model, where adversaries aim to infer sensitive information from shared model updates or blockchain transactions. The privacy objective is to prevent any leakage of raw data while ensuring that model updates remain secure.

To achieve this, the system utilizes:

1) **Local Training**: Data remains on IoT devices, ensuring that no raw data is transmitted to external entities.
2) **Secure Aggregation**: Model updates are aggregated using privacy-preserving techniques, mitigating the risk of individual contributions being exposed.
3) **Immutable Audit Trails**: Hyperledger Fabric ensures all transactions, including model updates, are logged immutably, enabling traceability without compromising privacy.

*2) Mathematical Privacy Proof:* We now formally prove that integrating Federated Learning with Hyperledger Fabric improves privacy by reducing the probability of sensitive data leakage.

**Theorem:** Let $\mathcal{D}_i$ represent the local dataset of IoT device $i$, and let $P_{\text{leak}}(\mathcal{D}_i)$ denote the probability of leakage of $\mathcal{D}_i$. When Federated Learning is combined with Hyperledger Fabric, $P_{\text{leak}}(\mathcal{D}_i)$ is minimized compared to traditional centralized machine learning frameworks.

**Proof:**

1) **Traditional Frameworks:** In centralized ML systems, raw data $\mathcal{D}_i$ is transmitted to a central server for model training. The probability of data leakage can be expressed as:

$$P_{\text{leak}}^{\text{centralized}}(\mathcal{D}_i) = P_{\text{comm}}(\mathcal{D}_i) + P_{\text{server}}(\mathcal{D}_i), \quad (1)$$

where $P_{\text{comm}}(\mathcal{D}_i)$ represents the probability of leakage during transmission, and $P_{\text{server}}(\mathcal{D}_i)$ represents the probability of leakage from the server due to breaches or attacks.

2) **Federated Learning:** In FL, raw data $\mathcal{D}_i$ remains on the device, and only model updates $\Delta w_i$ are transmitted. Thus:

$$P_{\text{leak}}^{\text{FL}}(\mathcal{D}_i) = P_{\text{comm}}(\Delta w_i) + P_{\text{agg}}(\Delta w_i), \quad (2)$$

where $P_{\text{agg}}(\Delta w_i)$ represents the probability of leakage during aggregation.

3) **Adding Blockchain:** By integrating Hyperledger Fabric, transactions related to model updates are immutably recorded, ensuring secure and traceable interactions. The blockchain employs encryption and access control, reducing $P_{\text{comm}}(\Delta w_i)$ and $P_{\text{agg}}(\Delta w_i)$ further:

$$P_{\text{leak}}^{\text{FL+Blockchain}}(\mathcal{D}_i) \leq \alpha P_{\text{comm}}(\Delta w_i) + \beta P_{\text{agg}}(\Delta w_i), \quad (3)$$

where $0 < \alpha, \beta < 1$ are reduction factors due to blockchain security mechanisms.

4) **Comparison:** Comparing probabilities:

$$P_{\text{leak}}^{\text{FL+Blockchain}}(\mathcal{D}_i) < P_{\text{leak}}^{\text{FL}}(\mathcal{D}_i) < P_{\text{leak}}^{\text{centralized}}(\mathcal{D}_i). \quad (4)$$

The inequality shows that combining FL with blockchain significantly reduces the probability of data leakage compared to both centralized ML and standalone FL systems.

The integration of Federated Learning with Hyperledger Fabric enhances privacy through local data retention, access control, secure transactions, and auditability, making the framework robust and suitable for privacy-sensitive IoT applications.

### B. Experimental analysis

*1) Simulation Setup:* To evaluate the performance and feasibility of the proposed system, we conducted simulations using a permissioned blockchain network implemented with Hyperledger Fabric v2.5.10. Table II outlines the parameters used in the simulation environment.

**TABLE II:** Simulation Parameters

| Parameter | Value |
|---|---|
| **Operating System** | Ubuntu 22.04.3 (64-bit) |
| **Blockchain Framework** | Hyperledger Fabric v2.5.10 |
| **Consensus Algorithm** | RAFT |
| **Number of Organizations** | 3 |
| **Number of Peers per Org** | 2 |
| **Channel Configuration** | 1 Channel |
| **Smart Contract Language** | Go |
| **Transaction Batch Size** | 10 |
| **Block Timeout** | 2 seconds |
| **Docker Environment** | Docker v24.0.7 |
| **Num. of Docker Containers** | 12 (Peers, Orderers, Services, Clients) |
| **Simulation Hardware** | Intel Core i7-7700HQ CPU, 6GB RAM |
| **Aggregation Algorithm** | Sequential Federated Averaging |

The simulation was performed on a single personal computer with the following specifications: an Intel Core i7-7700HQ CPU, 6GB of RAM, and a 64-bit Ubuntu operating system. This setup was used to emulate all nodes, services, and participants in the blockchain network and federated learning process. Despite the constraints of a single machine, the configuration was sufficient to simulate the proposed system under controlled conditions.

The blockchain framework was implemented using 12 Docker containers to manage peers, orderers, auxiliary services, and client applications. The network was organized into three organizations, each configured with two peers connected through a single channel. To ensure fault tolerance and consistency, the RAFT consensus algorithm was employed. Smart contracts, written in Go, were utilized to integrate federated learning with blockchain operations effectively. Transactions

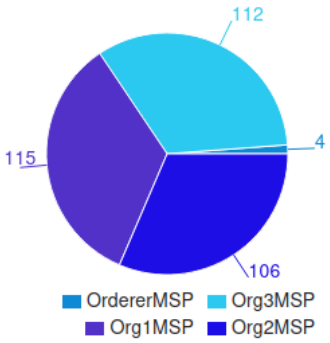


**Fig. 2:** Transactions by Organization in Hyperledger Fabric

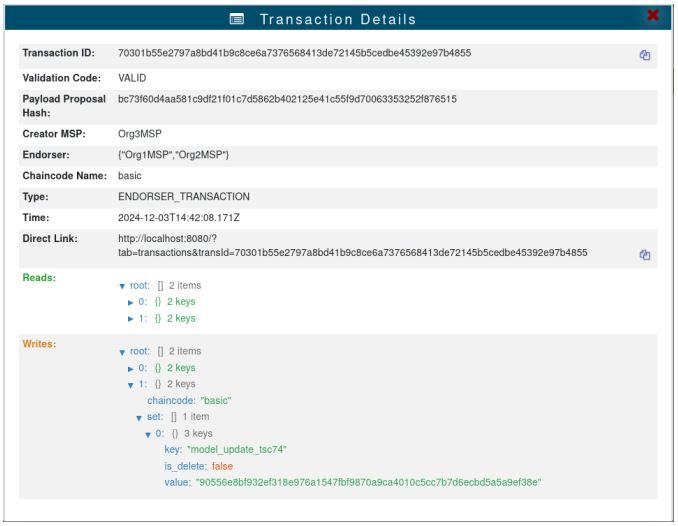


**Fig. 3:** Details of a Transaction in Hyperledger Fabric

were processed in batches of 10, with a block timeout set to 2 seconds to achieve a balance between throughput and latency.

Fig. 2 shows transactions per organization, and Fig. 3 details individual transactions in the Hyperledger Fabric framework. The federated learning process leveraged the Sequential Federated Averaging algorithm, which aggregated updates from distributed IoT devices simulated on the same machine.

The simulation provided insights into the interaction of the federated learning model with blockchain, focusing on key performance metrics such as transaction latency, throughput, and communication overhead.

*2) Results Evaluation:* To assess the efficiency of the proposed system model, we measured the average latency under different transaction arrival rates. The evaluation was conducted using a base Hyperledger Fabric network comprising three organizations, each with two peers. In each round, an equal number of transactions, representing model updates, were sent simultaneously from all three organizations. For example, when five concurrent transactions were sent from each organization, the total arrival rate was 15 concurrent transactions. This was repeated for arrival rates of 15, 30, 60, 120, 240, 480, and 960 transactions per second.

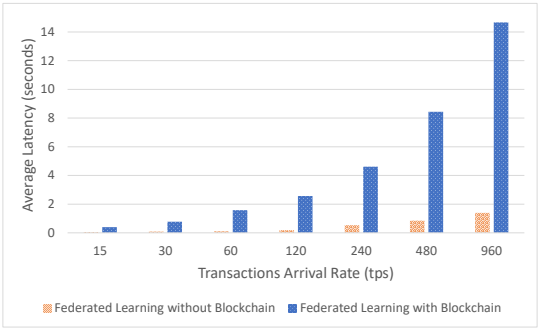


**Fig. 4:** Average Latency: FL with and without Blockchain

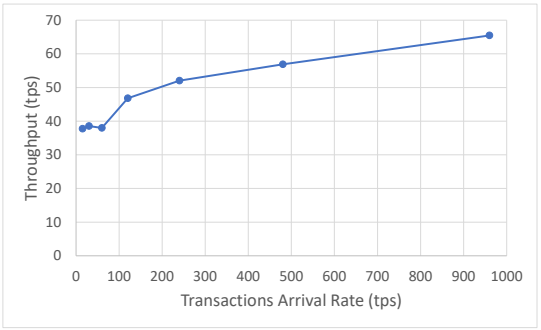


**Fig. 5:** Transaction Throughput at Different Arrival Rates

We measured two cases: 1. Federated learning without blockchain integration. 2. Federated learning with blockchain integration using Hyperledger Fabric.

The results demonstrate that integrating blockchain into federated learning introduces additional latency due to consensus and transaction validation processes. As shown in Fig. 4, the average latency increases with higher transaction arrival rates, with the gap between the two cases widening as the transaction load grows.

Specifically:

- For lower arrival rates (e.g., 15 tps), the latency for federated learning with blockchain is approximately 0.4 seconds, compared to 0.06 seconds without blockchain, indicating a minor overhead.
- At higher transaction rates, such as 960 tps, the latency for the blockchain-integrated system increases significantly to 14.6 seconds, while it remains relatively low (1.4 seconds) for the system without blockchain.

This trend highlights the scalability challenges introduced by blockchain integration under high transaction loads. However, the added latency is a trade-off for the enhanced security, transparency, and auditability provided by blockchain technology. These findings underscore the importance of optimizing blockchain parameters, such as block size and timeout, to minimize performance degradation.

A second graph, shown in Fig. 5, illustrates the throughput of the proposed system model. Throughput was measured as the number of transactions successfully processed per second for the same set of transaction arrival rates (15, 30, 60, 120, 240, 480, and 960). This throughput trend highlights the

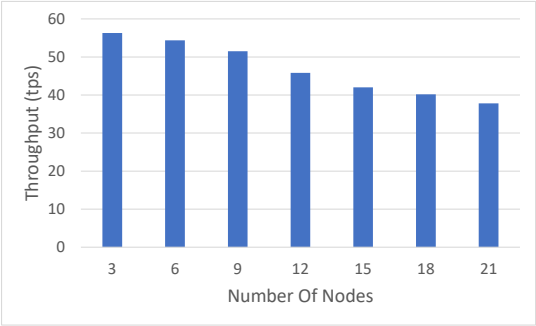


**Fig. 6:** Transaction Throughput for Varying Blockchain Network Sizes at 300 tps

system's ability to process transactions at various arrival rates while maintaining a robust throughput. As we can see, the throughput steadily increases as the transaction arrival rate grows, demonstrating the effective scalability of the proposed system model under increasing loads.

To further evaluate the scalability and performance of the proposed system model, we measured the throughput (tps) under varying numbers of blockchain nodes in the Hyperledger Fabric network. Starting with three nodes (one peer per organization), one peer was incrementally added to each of the three organizations at each step, resulting in configurations with 3, 6, 9, 12, 15, 18, and 21 nodes. The system was tested with a fixed transaction arrival rate of 300 transactions per second, and the results are shown in Fig. 6.

The results demonstrate the system's ability to sustain significant throughput even as the network size grows:

- At three nodes, the system achieved an initial throughput of 56.31 tps, indicating high efficiency in smaller network configurations.
- At nine nodes, throughput remained stable at 51.48 tps, showcasing the system's ability to handle larger deployments with minimal overhead.
- At 21 nodes, throughput was 37.79 tps, maintaining reasonable performance despite the increased complexity of a larger network.

It is important to note that these results were obtained from a simulation conducted on a single personal computer with limited computational and networking resources. In real-world scenarios, where each node operates on dedicated hardware with sufficient processing power and optimized networking, the system's throughput is expected to improve significantly. The observed trends provide a performance baseline and highlight the system's scalability potential under practical deployment conditions.

This analysis underscores the flexibility and applicability of the proposed federated learning system integrated with blockchain. It effectively balances decentralization, privacy, security, and performance, even when tested under constrained simulation environments.

## V. Conclusion and Future Work

This paper presented a blockchain-enabled federated learning framework leveraging Hyperledger Fabric to enhance privacy and security in IoT systems. The integration of blockchain's decentralized, tamper-proof capabilities with federated learning's data localization ensures secure model updates while preserving sensitive data. Our evaluation demonstrated improved data integrity, reduced leakage risks, and scalability, despite the performance overhead introduced by blockchain. Future efforts will focus on optimizing blockchain configurations, incorporating advanced privacy-preserving techniques, and adapting the framework for heterogeneous IoT environments. Real-world deployment and testing will further validate its effectiveness, paving the way for secure and decentralized machine learning in privacy-sensitive applications.

## References

[1] S. Munirathinam, "Chapter six - industry 4.0: Industrial internet of things (iiot)," in *The Digital Twin Paradigm for Smarter Systems and Environments: The Industry Use Cases* (P. Raj and P. Evangeline, eds.), vol. 117 of *Advances in Computers*, pp. 129–164, Elsevier, 2020.

[2] A. Karale, "The challenges of iot addressing security, ethics, privacy, and laws," *Internet of Things*, vol. 15, p. 100420, 2021.

[3] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. Vincent Poor, "Federated learning for internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1622–1658, 2021.

[4] J. Zhu, J. Cao, D. Saxena, S. Jiang, and H. Ferradi, "Blockchain-empowered federated learning: Challenges, solutions, and future directions," *ACM Comput. Surv.*, vol. 55, Feb. 2023.

[5] W. Issa, N. Moustafa, B. Turnbull, N. Sohrabi, and Z. Tari, "Blockchain-based federated learning for securing internet of things: A comprehensive survey," *ACM Comput. Surv.*, vol. 55, Jan. 2023.

[6] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*, EuroSys '18, (New York, NY, USA), Association for Computing Machinery, 2018.

[7] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, "Federated learning for internet of things: Recent advances, taxonomy, and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1759–1799, 2021.

[8] T. Zhang, L. Gao, C. He, M. Zhang, B. Krishnamachari, and A. S. Avestimehr, "Federated learning for the internet of things: Applications, challenges, and opportunities," *IEEE Internet of Things Magazine*, vol. 5, no. 1, pp. 24–29, 2022.

[9] S. Truex, N. Baracaldo, A. Anwar, T. Steinke, H. Ludwig, R. Zhang, and Y. Zhou, "A hybrid approach to privacy-preserving federated learning," in *Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security*, AISec'19, (New York, NY, USA), p. 1–11, Association for Computing Machinery, 2019.

[10] S. Banupriya and K. Kottilingam, "An analysis of privacy issues and solutions in public blockchain (bitcoin)," in *2021 2nd International Conference for Emerging Technology (INCET)*, pp. 1–7, 2021.

[11] H. Liu, D. Han, and D. Li, "Fabric-iot: A blockchain-based access control system in iot," *IEEE Access*, vol. 8, pp. 18207–18218, 2020.

[12] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, 2020.

[13] A. P. Kalapaaking, I. Khalil, and M. Atiquzzaman, "Smart policy control for securing federated learning management system," *IEEE Transactions on Network and Service Management*, vol. 20, no. 2, pp. 1600–1611, 2023.